REMARKS

Claims 1 through 33 were presented for examination and were pending in this application. In an Office Action dated October 21, 2004, claims 1 through 33 were rejected. Applicant thanks Examiner for examination of the claims pending in this application and addresses Examiner's comments below.

Applicant herein amends claims 1, 2, and 33. No claims are deleted or added. These changes merely correct ministerial errors such as improper spelling and transitions. They are believed not to introduce new matter and their entry is respectfully requested. The claims have been amended to expedite the prosecution of the application in a manner consistent with the Patent Office Business Goals, 65 Fed. Reg. 54603 (Sept. 8, 2000). In making this amendment, Applicant has not and does not narrow the scope of the protection to which Applicant considers the claimed invention to be entitled and does not concede that the subject matter of such claims was in fact disclosed or taught by the cited prior art. Rather, Applicant reserves the right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

Based on the following Remarks, Applicant respectfully requests that Examiner reconsider all outstanding objections and rejections, and withdraw them.

Response to Rejection Under 35 USC 103(a) in View of Chiu and Dietz

In the 4th paragraph of the Office Action, Examiner rejects claims 1 through 33 under 35 USC § 103(a) as allegedly being unpatentable in view of U.S. Patent No. 5,101,402 to Chiu et al. ("Chiu") and U.S. Patent No. 6,651,099 to Dietz et al. ("Dietz"). This rejection is respectfully traversed.

Claim 1 is directed to a method for providing unique identification of monitored network data instances flowing across various connections between networked devices. The unique identification is derived from information contained entirely within each instance of the network data. The method recites:

> using at least one monitoring device to monitor a network data instance flowing across at least one data connection;
>
> deriving from the data instance certain information which collectively provides a unique identification of the network data instance;
>
> assembling the derived information into an input string for a hash function; and
>
> using the output string of the hash function as a signature which represents a unique identifier of the network data instance.

Similarly, claim 18 is directed to an apparatus for providing unique identification of monitored network data instances flowing across various connections between networked devices. With the apparatus, the unique identification is derived from information contained entirely within each instance of the network data. The apparatus comprises:

> at least one monitoring device positioned to monitor a network data instance flowing across at least one data connection;
>
> a hash function device having an input string and an output string, the input string assembled from certain information derived from the network data instance, the information collectively providing a unique identification of the network data instance,
>
> wherein the output string is used as a signature which represents a unique identifier of the network data instance.

The claimed invention monitors a network and applies a hash function to provide a signature represents a network data instance. Hence, the claimed invention uniquely identifies a network data instance without a need to send a whole chunk of data across a network. This beneficially improves processing time and reduces network congestion. Further, the claimed invention also beneficially allows for tracking specific data instances between devices in a network. This allows for greater statistical accountability in a networked environment and also may be used to reduce or eliminate duplicative data along the network.

Neither Chiu nor Dietz, either alone or in combination, disclose, teach, or suggest the claimed invention. Chiu discloses a method to collect "information at the session level for a multiple node distributed processing system." *Chiu*, Abstract. In particular, a "first component software program monitors all packets passing through a node and extracts packet headers having a predetermined format from all nodes." *Id.* Thereafter, a "second component software program identifies a session in which each of the extracted packet headers was transmitted and, for each session, accumulates characterizing information about that session and calculates statistical data concerning all the sessions." *Id.* Chiu notes with respect to Figure 8c that "a unique session key is extracted for each session and serves to identify the packets of the session." *Id.*, col. 9, lines 3-5. While Chui discloses extraction of a unique identifier, as Examiner correctly notes, it fails to disclose creating a unique identifier using a hash function.

However, the shortcomings of Chiu are not rectified by Dietz. Dietz discloses a method for providing an identification of monitored network data that is <u>not</u> unique to each individual datum, or a network data instance. *See Dietz*, Abstract. Dietz does disclose use of an identifier for associating successively-received packets that are part of the same "flow." *Id.*, Abstract; col. 5, lines 25-34; col. 12, lines 6-11. In particular, Dietz discloses "extracting and information identifying (EII) engine that extracts selected parts of the packet, including identifying information from the packet as <u>required</u> for recognizing this packet as part of a flow." *Id.*, col. 13, lines 18-20 (emphasis added).

To rapidly identify whether a particular packet is part of a specific flow, the system in Dietz is configured to rapidly identify a packet signature to determine if it is a match to one associated with the specific flow. To accomplish this, Dietz discloses that a "slicer extracts important packet elements from the packet. These form a signature (i.e., key) for the packet. The slicer also preferably generates a hash for rapidly identifying a flow that may have this signature from a database of known flows." *Id.*, col. 6, lines 13-19. Hence, the hash disclosed in Dietz is <u>not</u> the signature or even part of the signature. Rather, it is information passed on for the system to use for comparison with signatures. The hash is not independent of the signature; instead, it is used to identify packets that might have the same signature as other packets in a flow. The signature and the hash are functionally distinct from each other. In contrast, the claimed invention computes a hash that <u>is</u> the identifying signature.

Since Dietz fails to disclose at least the steps of "assembling the derived information into an input string for a hash function" and "using the output string of the hash function as a signature which represents a unique identifer of the network data instance," as well as the elements of "a hash function device having an input string and an output string, the input string assembled from certain information derived from the network data instance, the information collectively providing a unique identification of the network data instance, wherein the output string is used as a signature which represents a unique identifier of the network data instance," it fails to remedy the deficiencies of Chiu. Therefore, the combination of Chiu and Dietz fails to disclose Applicant's claimed invention and Applicant respectfully submits that claims 1 and 18 are patentably distinguishable over the cited references.

As for claims 2 though 17 and 19 through 33, these recite additional patentable features of the claimed invention that are not disclosed or suggested by Chiu or Dietz, either alone or in combination. With respect to claims 2, 7 through 9, and 24 through 26, Chiu merely discloses conventional header and packet information, which includes initiation and destination node addresses. *See Chiu*, col., 8, lines 40-65. This is not what Applicant claims. Rather, Applicant's claimed invention recites, e.g., "deriving from the data instance a source and destination address for the data," "deriving from the data instance a source and destination port associated with the networked devices," and "deriving from the data instance at least one sequence number associated with data instance," for use as an input string for the hash function to output a signature that is a unique identifier for the network data instance. As previously stated, Chiu fails to use such packet information and Dietz fails to use a hash function as a signature. Thus, for at least this reason claims 2, 7 through 9, and 24 through 26 are patentably distinguishable over the cited references.

With respect to claims 3, 4, 15, 20, 21, and 32 (as well as claims 5, 6, 10, 22, 23, and 27), as noted previously, both Chiu and Dietz fail to disclose a signature as claimed by Applicant. Hence, because neither reference uses, for example, a hash function as a signature, neither reference discloses, e.g., "attaching the signature to at least one data report associated with the network data instance" and "transmitting the data reports and signatures from each monitoring device to a central collecting device." Thus, for at least this reason claims 3, 4, 15, 20, 21, and 32 (and claims 5, 6, 10, 22, 23, and 27) are patentably distinguishable over the cited references.

In summary, Applicant respectfully requests reconsideration and removal of the basis of the reject to claims 1 through 33. Applicant also requests allowance of these claims at this time.

Conclusion

Applicant is also submitting herewith an information disclosure statement with additional cited references. Applicant respectfully submits the claimed invention is patentably distinguishable over these cited references.

In sum, Applicant respectfully submits that claims 1 through 33, as presented herein, are patentably distinguishable over the cited references (including references cited, but not applied). Therefore, Applicant requests reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicant respectfully invites Examiner to contact Applicant's representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Leslie V. Niles

Date: February 22, 2005

By: Raj P Patel

Rajiv P. Patel, Attorney of Record
Registration No. 39,327
FENWICK &,WEST LLP
801 California Street
Mountain View, CA 94041
Phone: (650) 335-7607
Fax: (650) 938-5200